In the Specification:

Amend the paragraph on page 4, spanning lines 21 and 22, as shown below:

Fig. 3 is a block diagram illustrating an exemplary filter set and exemplary virtualization data in accordance with certain ~~embodiment~~ embodiments of the invention.

Amend the paragraph on page 10, spanning lines 8 through 19, as shown below:

Controller 112 may also optionally maintain a log or other record (not shown) of data packets that were not allowed to pass through the network mediator. This record may be a copy of the entire data packet, or alternatively only selected parts of the data packet (e.g., source and/or destination address, data packet protocol, etc.). Additional information may also be maintained, such as a timestamp indicating the date and time the data packet was received, which filter was the cause of the refusal to allow the packet through, etc. Such information can then be used for a variety of different ~~manners~~ purposes. For example, the information could be examined to try to identify if a malicious user or program is attempting to break into a particular computing device(s), or to identify an improperly functioning program that, due to an error in the program, is attempting to access computing devices it should not be (e.g., during a debugging process), etc.

Amend the paragraph spanning page 13, line 18, through page 14, line 3, as shown below:

Fig. 3 is a block diagram illustrating an example filter set and virtualization data in accordance with certain ~~embodiment~~ embodiments of the invention. The filter set and virtualization data 160 of Fig. 3 are discussed with additional reference to components in Fig. 1. Although the filter set and virtualization data 160 are illustrated in a table format for ease of illustration, it is to be appreciated that filters and virtualization data 160 can be maintained at a network mediator 108 or 110 using any of a wide variety of conventional data structures. Furthermore, the filter set and virtualization data 160 are illustrated with reference to Internet Protocol (IP) data packet filtering. Alternatively, data packets can be filtered for different protocols, with the parameters of the filters varying based on the protocol (e.g., there would be no port parameters if the protocol did not support ports).

Amend the paragraph on page 17, spanning lines 1 through 9, as shown below:

The nodes 210 are grouped together in clusters, referred to as server clusters (or node clusters). For ease of explanation and to avoid cluttering the drawings, only a single cluster 212 is illustrated in Fig. 4. Each server cluster includes nodes 210 that correspond to a particular customer of co-location facility [[104]] 208. The nodes 210 of a server cluster are physically isolated from the nodes 210 of other server clusters. This physical isolation can take different forms, such as separate locked cages or separate rooms at co-location facility [[104]] 208. Physically isolating server clusters ensures customers of co-location facility [[104]] 208 that only they can physically access their nodes (other customers cannot).

Amend the paragraph on page 17, spanning lines 10 through 18, as shown below:

A landlord/tenant relationship (also referred to as a lessor/lessee relationship) can also be established based on the nodes 210. The owner (and/or operator) of co-location facility [[104]] 208 owns (or otherwise has rights to) the individual nodes 210, and thus can be viewed as a "landlord". The customers of co-location facility [[104]] 208 lease the nodes 210 from the landlord, and thus each can be viewed as a "tenant". The landlord is typically not concerned with what types of data or programs are being stored at the nodes 210 by the tenant, but does impose boundaries on the clusters that prevent nodes 210 from different clusters from communicating with one another, as discussed in more detail below.

Amend the paragraph spanning page 18, line 20 through page 19, line 7, as shown below:

Co-location facility [[104]] 208 supplies reliable power 214 and reliable network connection(s) 216 to each of the nodes 210. Power 214 and network connection(s) 216 are shared by all of the nodes 210, although alternatively separate power 214 and network connection(s) 216 may be supplied to nodes 210 or groupings (e.g., clusters) of nodes. Any of a wide variety of conventional mechanisms for supplying reliable power can be used to supply reliable power 214, such as power received from a public utility company along with backup generators in the event of power failures, redundant generators, batteries, fuel cells, or other power storage mechanisms, etc. Similarly, any of a wide variety of conventional mechanisms for supplying a reliable network connection can be used to supply network connection(s) 216, such as redundant connection transport media, different types of connection media, different access points (e.g., different Internet access points, different Internet service providers (ISPs), etc.).

Amend the paragraph on page 21, spanning lines 10 through 20, as shown below:

Cluster operations management console 240 also establishes cluster boundaries within co-location facility 208 by adding filters to the network mediator corresponding to each node 210 that allows the node to communicate only with other nodes in its cluster. The cluster boundaries established by console 240 prevent nodes 210 in one cluster (e.g., cluster 212) from communicating with nodes in another cluster (e.g., any node not in cluster 212), while at the same time not interfering with the ability of nodes 210 within a cluster from communicating with other nodes within that cluster. These boundaries provide security for the tenants' data, allowing them to know that their data cannot be communicated to other tenants' nodes 210 at facility [[104]] 208 even though network connection 216 may be shared by the tenants.

Amend the paragraph spanning page 21, line 21, through page 22, line 4, as shown below:

In the illustrated example, each cluster of co-location facility [[104]] 208 includes a dedicated cluster operations management console. Alternatively, a single cluster operations management console may correspond to, and manage hardware operations of, multiple server clusters. According to another alternative, multiple cluster operations management consoles may correspond to, and manage hardware operations of, a single server cluster. Such multiple consoles can manage a single server cluster in a shared manner, or one console may operate as a backup for another console (e.g., providing increased reliability through redundancy, to allow for maintenance, etc.).

Amend the paragraph on page 27, spanning lines 10 through 19, as shown below:

Software engines 252 include any of a wide variety of conventional software components. Examples of engines 252 include an operating system (e.g., the Windows NT® operating system), a load balancing server component (e.g., to balance the processing load of multiple nodes 210), a caching server component (e.g., to cache data and/or instructions from another node 210 or received via the Internet), a storage manager component (e.g., to manage storage of data from nodes 210 received via the Internet), etc. In one implementation, each of the engines 252 is a protocol-based engine, communicating with BMonitor 250 and other engines 252 via messages and/or function calls without requiring the engines 252 and BMonitor 250 to be written using the same programming language.

Amend the paragraph spanning page 27, line 20, through page 28, line 5, as shown below:

Controller 254 may optionally be further responsible for controlling the execution of engines 252. This control can take different forms, including beginning execution of an engine 252, terminating execution of an engine 252, re-loading an image of an engine 252 from a storage device, etc. Controller 254 receives instructions from application operations management console 242 of Fig. 4 regarding which of these control actions to take and when to take them. Thus, the control of engines 252 is actually managed by the remote application operations management console 242, not locally at co-location facility [[104]] 208. Controller 254 also provides an interface via which application operations management console 242 can identify filters to add (and/or remove) from filter set 114 ~~258~~.

Amend the paragraph spanning page 48, line 2 to page 49, line 2 as shown below:

~~Packet filters and network virtualization are used to restrict network communications.~~ A network mediator corresponding to a computing device uses packet filters to restrict network communications. The network mediator includes a set of one or more filters, each filter having parameters that are compared to corresponding parameters of a data packet to be passed through the network mediator ~~(either from or to the computing device)~~. The network mediator determines whether to allow the data packet through based on whether the data packet parameters match any filter parameters. The set of filters can be modified by a remote device, but cannot be modified by the computing device whose communications are being restricted ~~(thereby preventing the device whose communications are being restricted from being able to modify those restrictions)~~. ~~Additionally, the set of filters may be modified by remote devices at different managerial levels, although remote devices are prohibited from modifying filters to make the filters less restrictive than filters imposed by higher level devices. Network virtualization can be also be used, either in addition to or in combination with the packet filters, to restrict network communications by the network mediator maintaining a mapping of virtual addresses to network addresses, and allowing the computing device to access only the virtual addresses.~~ When a data packet is sent from the computing device, the data packet will include the virtual address which is changed to the network address by the network mediator prior to forwarding the packet on the network, and vice versa. ~~Similarly, when a data packet is received at the network mediator targeting the computing device, the~~

~~network mediator changes the network address in the data packet to the corresponding virtual address.~~ By virtualizing the addresses, the computing device is restricted in ~~its knowledge and ability to access~~ accessing other devices over the network ~~because it has no knowledge of what the other devices' addresses are~~.